תורת המספרים האנליטית, מחנה קיץ 2015 / אופיר גורודצקי

0. מבוא

תורת המספרים האנליטית היא נקודת המפגש של תורת המספרים ואנליזה. בתחום זה שואלים (ועונים) על שאלות כמותיות, שהן לרוב קשות בהרבה משאלות איכותיות. השאלה הקלאסית, וגם זו שנתמקד בה בהרצאה, היא: **כמה ראשוניים יש עד x?** על שאלה זו ענו, באופן חלקי, בסוף המאה ה־19 ("משפט המספרים הראשוניים"). רק באופן חלקי, משום שהשערת רימן, שעודה פתוחה, גורסת שהקירוב שהוכיחו הוא הרבה יותר "טוב" ממה שיודעים להוכיח עם הכלים הנוכחיים.

שאלות קשות יותר שאפשר לשאלות בעקבות זו הן: כמה ראשוניים עד x יש בסדרה חשבונית נתונה? (גם נפתרה חלקית) וכמה ראשוניים יש בקטע $[x,y]$? (נחקר עד ימינו, ולא תמיד נובע מהשערת רימן).

יש מגוון שלם של שאלות אדיטיביות שלא נתעסק בהן בהרצאה זו (השערת גולדבאך, השערת הראשוניים התאומים, משפט ווירינג, ועוד), על אף שניתן להתקדם בהן הרבה באופן אלמנטרי.

1. בנייה (אוקלידס)

הגדרה: ראשוני ־ מספר טבעי גדול מ־1 שמחלקיו הם רק הוא עצמו ו־1.

המשפט היסודי של האריתמטיקה (אוקלידס, "יסודות", $\sim$300 לפנה"ס): כל מספר טבעי אפשר לכתוב כמכפלה של מספרים ראשוניים, באופן יחיד עד כדי שינוי סדר.

מסקנה: מספר p הוא ראשוני אמ"מ $\forall a,b\in\mathbb{N}:\ p\mid ab\implies p\mid a\vee p\mid b$.

אוקלידס ענה גם השאלה הבאה:

משפט: יש אינסוף ראשוניים. הוכחה: נבנה סדרת ראשוניים עולה $\{p_n\}_{n=1}^{\infty}$, באינדוקציה. $p_1:=2$, ובהינתן $p_1,\cdots,p_n$ נגדיר את p_{n+1} להיות גורם ראשוני של $P_n:=p_1\cdot p_2\cdot\cdots\cdot p_n+1$ (לא משנה איזה, נניח הקטן ביותר). בהכרח יש כזה כי המכפלה גדולה ממש מ־1, והוא בהכרח שונה מהקודמים כי שארית החלוקה של P_n ב־p_i ($i\le n$) שונה מ־0 (ספציפית, שווה 1). ■

הערה: יש המנסחים הוכחה זו כהוכחה בשלילה. זה לא נכון היסטורית ובעיקר מיותר.

תשובה זו עדיין לא מניחה את דעתנו. נרצה לקבל הערכה כמותית למספר הראשוניים עד x[1]. נכניס סימון סטנדרטי: $\pi(x):=|\{n\le x:\ n\text{ is prime}\}|$ (כל שאנו יודעים בינתיים זה $\pi(x)\xrightarrow[x\to\infty]{}\infty$). הנה תוצאה כמותית ראשונה:

טענה: לכל $x>1$ מתקיים $\pi(x)\ge\ln\ln x+O(1)$. הוכחה: מהוכחה של אוקלידס, ניתן להראות באינדוקציה כי הראשוני ה־n־י בגודלו קטן/שווה 2^{2^n}. על כן $\pi(x)\ge\pi(2^{2^{\lfloor\log_2\log_2 x\rfloor}})\ge\lfloor\log_2\log_2 x\rfloor\ge\ln\ln x+O(1)$. ■

2. הכלה־הדחה (ארטוסתנס, אוילר ולז'נדר)

הנפה של ארטוסתנס (276־194 לפנה"ס) היא אלגוריתם למציאת כל הראשוניים בין 1 ל־n. הרעיון הוא זה: נכתוב את המספרים 2 עד n בשורה. ניקח את המספר הקטן ביותר בשורה (2), שהוא בהכרח ראשוני. נמחק מהרשימה את כל הכפולות שלו, לא כולל הוא עצמו (הן מספרים פריקים). נעבור למספר הבא במערך שלא נמחק עדיין (3) ־ הוא בהכרח ראשוני, נמחק את כפולותיו, לא כולל הוא עצמו. וכן הלאה, עד שהגענו למספר האחרון ברשימה. בסוף התהליך אנחנו נשארים עם כל המספרים הראשוניים עד n, ורק איתם.

[1] כל החישובים שנעשה יניחו ש־x מספר טבעי. עם זאת, גם אם הוא סתם מספר ממשי חיובי, רוב החישובים ישארו נכונים.

הבחנה: מספיק לנפות על כפולות ראשוניים עד $\lfloor\sqrt{x}\rfloor$, מהסיבה שלכל מספר פריק יש גורם ראשוני קטן או שווה מהשורש שלו, ובטווח שלנו זה גורר שהוא קטן/שווה $\sqrt{x}$.

לז'נדר הבין ב־1808 שאפשר לתרגם אלגוריתם זה, עם שינויים קלים, לחסם עליון על $\pi(x)$. נשתמש בנפה על הטבעיים מ־2 עד x, אך ננפה רק כפולות של ראשוניים **עד** z (כולל כפולות של z, אם הוא ראשוני), כאשר z הוא פרמטר קטן מ־x שיקבע בהמשך. לשם הנוחות, הפעם נמחק גם את הראשוניים עד z, ולא רק את כפולותיהם.

לאחר הניפוי החלקי הזה נישאר רק עם מספרים שמחלקיהם הראשוניים גדולים ממש מ־z. בפרט, נקבל את כל הראשוניים בין z ל־x - אלו $\pi(x)-\pi(z)$ מספרים לפחות.

אפשר להביע את כמות המספרים שנותרו באופן הבא: $(x-1)$ מספרים התחלתיים פחות $\lfloor\frac{x}{p}\rfloor$ כפולות של p בין 2 ל־x) ועוד $\sum_{p\le z,p\text{ prime}}\lfloor\frac{x}{p}\rfloor$ (כי מספרים שמתחלקים בשני ראשוניים קטנים/שווים z ספרנו פעמיים), וכן הלאה.

נמשיך בהכלה־הדחה זו ונקבל סכום גדול שמכיל $2^{\pi(z)}$ מחוברים - אחד לכל תת־קבוצה של הראשוניים עד z. ספציפית, עבור סדרת ראשונים $p_1>p_2>\cdots>p_k\le z$, יופיע המחובר $\lfloor\frac{x}{p_1\cdot\cdots\cdot p_k}\rfloor$ עם הסימן $(-1)^k$ (יוצא הדופן הוא המקרה של אוסף ראשוניים ריק, קרי $k=0$, עבורו יופיע המחובר $x-1$). מחובר זה ניתן לקרב ע"י $\frac{x}{p_1\cdot\cdots\cdot p_k}$ ועוד שגיאה קטנה ממש מ־1.

כזכור, אמרנו שהתוצאה היא לפחות $\pi(x)-\pi(z)$ מספרים, על כן:

$$\begin{aligned}\pi(x)-\pi(z) &\le -1+2^{\pi(z)}+x-\sum_{p_1\le z}\frac{x}{p_1}+\sum_{p_1<p_2\le z}\frac{x}{p_1p_2}\mp\cdots\\ &= -1+2^{\pi(z)}+x\prod_{p\le z}(1-\frac{1}{p})\end{aligned}$$

כאשר הגורם $2^{\pi(z)}$ הוא חסם עליון על סכום כל השגיאות. כעת נשתמש בחסם הטריוויאלי $\pi(z)\le z$ ונקבל: $\pi(x)\le z-1+2^z+x\prod_{p\le z}(1-\frac{1}{p})$.

למה (אוילר): $\frac{1}{\ln z}\le\prod_{p\le z}(1-\frac{1}{p})$. הוכחה: $\ln z\ge\sum_{n\le z}\frac{1}{n}\ge\prod_{p\le z}(1-\frac{1}{p})^{-1}$. ■

על כן $\pi(x)\le z-1+2^z+\frac{x}{\ln z}$. אם נבחר $z=\ln x$, נקבל $\pi(x)\le\frac{x}{\ln\ln x}+O(x^{\ln 2})$. ■

מסקנה: צפיפות הראשוניים היא 0: $\lim_{x\to\infty}\frac{\pi(x)}{x}=0$. ■

הערה: כדאי לציין שעל אף ששיפרו את החישוב הנ"ל עד מאוד בדרכים שונות (ברון וסלברג הם שני שמות חשובים בהקשר זה), הוא מאפשר לקבל רק חסמים עליונים על $\pi(x)$.

3. עצרת (צ'בישב, מרטנס) n

ב־1798 לז'נדר שיער, מתוך התבוננות בערכי $\pi(x)$, ש־$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}=1$. כלומר, הסיכוי שמספר יהיה ראשוני פרופורציוני להופכי של כמות הספרות שלו.

ב־1850 צ'בישב הוכיח כי $\pi(x)=\theta(\frac{x}{\ln x})$ (תוצאה מדוייקת בהרבה ממה שקיבלנו עד כה), ושאם קיים הגבול $\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}$ אז הוא שווה ל־1.

ב־1859 רימן הסביר איך תחת הנחות מסויימות על הפונקציה $\zeta(s) := \sum_{n\geq 1} n^{-s}$ (במשתנה מרוכב s) ניתן להוכיח את ההשערה של לז'נדר. ב־1896 הוכיחו סוף־סוף הדמר וואלי פוסן את ההשערה (באופן בלתי תלוי), שידועה כיום בתור "משפט המספרים הראשוניים" (Prime Number Theorem - PNT). ב־1948 סיפקו סלברג וארדש (באופן תלוי) לראשונה הוכחה אלמנטרית נטולת־מרוכבים למשפט.

בפרק זה נפרט על חלק מהתוצאות של צ'בישב ושל מרטנס, שמתקרבות ל־PNT. כל ההוכחות יהיו קשורות ל־$n!$ ולמקדמים בינומים. נעבוד בעיקר עם פונקציות ממושקלות:

$$\begin{aligned}\vartheta(x) &:= \sum_{p\leq x} \ln p \\ \psi(x) &:= \sum_{p^k\leq x} \ln p = \sum_{k\geq 1} \vartheta(x^{1/k}) = \vartheta(x) + O(\sqrt{x}\ln x)\end{aligned}$$

מסתבר שכל מידע עליהן אפשר להמיר למידע על $\pi(x) = \sum_{p\leq x} 1$, נראה זאת בהמשך.

נפתח בכמה למות טכניות:

<u>למה (קירוב ע"י אינטגרל):</u> אם f פונקציה רציפה ב־$[1,\infty)$ ומונוטונית, אז $\sum_{n=1}^{N} f(n) = \int_1^N f(x)dx + O(\max\{|f(1)|, |f(N)|\})$. <u>הוכחה:</u>

$$\sum_{n=1}^{N} f(n) - \int_1^N f(x)dx = f(N) + \sum_{n=1}^{N-1}(f(n) - \int_n^{n+1} f(x)dx)$$

אם f עולה, הסכום אי־חיובי וחסום מלמטה ע"י $\sum_{n=1}^{N-1}(f(n) - f(n+1)) = f(1) - f(N)$. אם f יורדת, הסכום אי־שלילי וחסום מלמעלה ע"י $\sum_{n=1}^{N-1}(f(n) - f(n+1)) = f(1) - f(N)$. ■

<u>מסקנה ("בייבי סטירלינג"):</u> $\ln(n!) = n\ln n - n + O(\ln n)$. <u>הוכחה:</u> נציב בלמה $f(x) = \ln x$, וניזכר שהפונקציה הקדומה של $\ln x$ היא $x\ln x - x$. ■

<u>למה ("בייבי סטירלינג" 2):</u> $\frac{4^n}{\sqrt{n+1}} < \binom{2n}{n}$. <u>הוכחה:</u> $\frac{1}{\sqrt{n+1}} = \frac{1}{\sqrt{n+1}} < \prod_{i\leq n}\sqrt{1-\frac{1}{i+1}} = \prod_{i\leq n}(1-\frac{1}{2i}) = \frac{\binom{2n}{n}}{4^n}$. ■

נתחיל עם החסם העליון הבא:

<u>משפט (צ'בישב):</u> $\vartheta(x) = O(x)$, עם קבוע $\ln 4$. <u>הוכחה:</u> $\binom{2n}{n}$ מתחלק בכל הראשוניים ב־$[n+1, 2n-1]$. לכן $\prod_{n<p<2n} p < \frac{4^n}{\sqrt{n+1}}$, ובאינדוקציה חזקה $\forall n \geq 2 : \prod_{p\leq n} p < 4^n$. כעת ניקח לוג. ■

<u>מסקנה:</u> $\pi(x) = O(\frac{x}{\ln x})$. <u>הוכחה:</u> לכל $\varepsilon \in (0,1)$, מתקיים:

$$\vartheta(x) \geq \ln(x^\varepsilon)(\pi(x) - \pi(x^\varepsilon)) = \varepsilon\ln x\pi(x) + O(x^\varepsilon \ln x)$$

כלומר $\pi(x) \leq \frac{\vartheta(x)+O(x^\varepsilon\ln x)}{\varepsilon\ln x} = \frac{\vartheta(x)}{\varepsilon\ln x} + O(x^\varepsilon) = O(\frac{x}{\ln x})$. אפשר לקחת את הקבוע להיות קרוב כרצוננו ל־$4\ln$. ■

אפשר עם אותו רעיון וקצת יותר מאמץ לקבל גם חסם תחתון, אנחנו דוחים זאת לפרק הבא.

<u>משפט (מרטנס):</u> $\sum_{p\leq x} \frac{\ln p}{p} = \ln x + O(1)$. <u>הוכחה:</u> נשתמש בפירוק של $n!$ (לז'נדר): $n! = \prod_{p\leq n} p^{\sum_{k\geq 1}\lfloor n/p^k\rfloor}$. בזכות זה ש־$\ln(n!) = n\ln n + O(n)$ ו־$\sum_{k\geq 1}\lfloor n/p^k\rfloor = \frac{n}{p} + O(1) + O(\frac{n}{p^2})$, ניקח לוג ונקבל:

$$n\ln n+O(n)=\sum_{p\le n}\ln p(\frac{n}{p}+O(1)+O(\frac{n}{p^2}))$$

נחלק ב־n:

$$\ln n+O(1)=\sum_{p\le n}\frac{\ln p}{p}+O(\frac{\sum_{p\le n}\ln p}{n})+O(\sum_{p\le n}\frac{\ln p}{p^2})$$

הסכום $\frac{\sum_{p\le n}\ln p}{n}$ חסום לפי המשפט הקודם, והטור $\sum_p\frac{\ln p}{p^2}$ סופי כי הטור $\sum_n\frac{\ln n}{n^2}$ מתכנס. נובע $\sum_{p\le n}\frac{\ln p}{p}=\ln n+O(1)$. ■

<u>מסקנה:</u> $\sum_{p\le x}\frac{1}{p}=\ln\ln x+O(1)$. <u>הוכחה:</u> נתחיל בלהציג שיוויון יפהפה של אבל (Abel) שמזכיר אינטגרציה בחלקים מהסיבה שהוא מהווה אינטגרציה בחלקים:

$$\sum_{n\le x}a_nb_n=(\sum_{n\le x}a_n)b_x-\sum_{n\le x-1}(\sum_{m\le n}a_m)(b_{n+1}-b_n)$$

אם נבחר $a_n=\frac{\ln n}{n}\cdot 1_{n\text{ is prime}},b_n=\frac{1}{\ln n}$, נקבל:

$$\sum_{p\le x}\frac{1}{p}=(\sum_{p\le x}\frac{\ln p}{p})\frac{1}{\ln x}+\sum_{n\le x-1}(\sum_{p\le n}\frac{\ln p}{p})\frac{\ln(n+1)-\ln n}{\ln n\ln(n+1)}$$

נציב $\sum_{p\le n}\frac{\ln p}{p}=\ln n+O(1)$. נפשט בעזרת $\ln(1+\frac{1}{n})=\frac{1}{n}+O(\frac{1}{n^2})$ וגם בעזרת הקירוב $\sum_{n\le x}\frac{1}{n\ln n}=\int_{n\le x}\frac{dx}{x\ln x}+O(1)=\ln\ln x+O(1)$. השגיאות יוצאות $O(1)$ כי הטורים $\sum\frac{1}{n\ln^2 n},\sum\frac{1}{n^2\ln n}$ מתכנסים.■

<u>מסקנה:</u> $\prod_{p\le x}(1-\frac{1}{p})=\frac{e^{O(1)}}{\ln x}$. <u>הוכחה:</u> נכתוב $1-\frac{1}{p}=e^{-\frac{1}{p}+O(\frac{1}{p^2})}$. המכפלה נהיית $e^{-\sum_{p\le x}\frac{1}{p}+O(1)}=\frac{e^{O(1)}}{e^{\ln\ln x}}=\frac{e^{O(1)}}{\ln x}$. ■

<u>משפט (צ'בישב):</u> אם קיים הגבול $\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}$, אז הוא שווה 1. <u>הוכחה:</u> ראשית, אם גבול זה קיים אז קיים גם הגבול $\lim_{x\to\infty}\frac{\vartheta(x)}{x}$ ושווה לו, כי

$$\pi(x)\ln x\ge\vartheta(x)\ge\varepsilon\ln x\pi(x)+O(x^\varepsilon\ln x)$$

שנית, אפשר להשתמש שוב בסכימה של אבל, עם $a_n=\ln n\cdot 1_{n\text{ is prime}},b_n=\frac{1}{n}$:

$$\sum_{p\le x}\frac{\ln p}{p}=\frac{\vartheta(x)}{x}+\sum_{i\le x-1}\frac{\vartheta(i)}{i(i+1)}$$

לפי $\vartheta(x)=O(x)$ ו־$\sum_{p\le x}\frac{\ln p}{p}=\ln x+O(1)$, נובע $\sum_{i\le x-1}\frac{\vartheta(i)}{i(i+1)}=\ln x+O(1)$. אם $L=\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}$ גדול מ־1 אז $L=\lim_{x\to\infty}\frac{\vartheta(x)}{x}$ גדול מ־1 ולכן $\vartheta(i)>\frac{L+1}{2}i$ לכל i גדול מספיק, ונובע שהסכום האחרון גדול מ־$\sum_{i\le x-1}\frac{L+1}{2(i+1)}+O(1)=\frac{L+1}{2}\ln x+O(1)$, סתירה. כנ"ל אם $L<1$. ■

זה מקום לכמה הערות:

<u>הערה 1:</u> למעשה, מרטנס הראה ש־$\prod_{p\le x}(1-\frac{1}{p})=\frac{e^\gamma}{\ln x}(1+o(1))$. זה גורם לנו להבין משהו מדכא לגבי הנפה של ארטוסתנס. ראינו בסעיף השני שאם מנפים כפולות של ראשוניים עד סף z, מקבלים את כל הראשוניים בין z ל־x (ואולי כמה מספרים פריקים), כלומר מקבלים לפחות $\pi(x)-\pi(z)$ מספרים. מצד שני, הצגנו ביטוי זה בתור $x\prod_{p\le z}(1-\frac{1}{p})$ ועוד "שגיאה" שנסמן ב־$E(x,z)$. הסברנו שלז'נדר בחר סף $z=\ln x$ שאיפשר לו להראות שהשגיאה $E(x,z)$ זניחה לעומת המכפלה $x\prod_{p\le z}(1-\frac{1}{p})$.

העניין הוא שגם אם עובדים עם הסף האידאלי $z = \lfloor\sqrt{x}\rfloor$ שנותן את השיוויון $\pi(x) - \pi(\lfloor\sqrt{x}\rfloor) = x\prod_{p\le z}(1-\frac{1}{p}) + E(x,z)$, השגיאה E אינה זניחה לעומת המכפלה, מכיוון שהתוצאה השלישית של מרטנס אומרת שהביטוי $x\prod_{p\le\sqrt{x}}(1-\frac{1}{p})$ אסימפטוטי ל־$2e^{-\gamma}\frac{x}{\ln x}$, והקבוע $2e^{-\gamma}$ גדול מעט מ־1, שהוא הקבוע שצריך להופיע על פי משפט המספרים הראשוניים: $\pi(x) - \pi(\lfloor\sqrt{x}\rfloor) \sim \frac{x}{\ln x}$. לכן אי־אפשר להתייחס לשגיאה E בתור "$O(E)$", חייבים לנתח אותה במדויק כאילו היא איבר מרכזי, ואין דרך פשוטה לעשות זאת...

<u>הערה 2:</u> ההוכחה המקורית של מרטנס הייתה מתוחכמת ומדויקת בהרבה והשתמשה בפונקציית זטא. עם זאת, היא לא הייתה מדויקת "מידי" כי חישוב מדויק דורש את משפט המספרים הראשוניים.

<u>הערה 3:</u> אפשר לחקור גם פולינומים ראשוניים מעל שדה סופי $\mathbb{F}_p$. האנלוג שם לפונקציית העצרת הוא $x - x^{p^n}$ - פולינום קסום שמתחלק בכל הראשוניים ממעלה המחלקת את n.

נסיים את הפרק בשני שיקולים היוריסטיים שונים שמסביר מדוע נצפה ש־$\pi(x) \sim \frac{x}{\ln x}$.

<u>שיקול 1:</u> אם ננפה כפולות של ראשוניים עד שורש x בקטע $[1,x]$, נישאר בערך עם $\pi(x) - \pi(\sqrt{x}) \sim \pi(x)$ מספרים. מצד שני, זה שווה בערך ל־$x\prod_{p\le\sqrt{x}}(1-\frac{1}{p})$, כי הסיכוי שמספר לא מתחלק ב־p הוא $1-\frac{1}{p}$ ומאורעות אלה הם בלתי־תלויים (בקירוב). נקבל:

$$\pi(x) \sim x\prod_{p\le\sqrt{x}}(1-\tfrac{1}{p}) \sim xe^{-\sum_{p\le\sqrt{x}}\frac{1}{p}}$$

מתוך סכימת אבל, נקבל: $\sum_{p\le\sqrt{x}}\frac{1}{p} \sim \frac{\pi(\sqrt{x})}{x} + \sum_{i\le\sqrt{x}}\frac{\pi(i)}{i^2} \sim \sum_{i\le\sqrt{x}}\frac{\pi(i)}{i^2}$. אם ניקח לוג נקבל: $\ln\frac{\pi(x)}{x} \sim -\sum_{i\le\sqrt{x}}\frac{\pi(i)}{i^2}$. נסמן $f(t) := \frac{\pi(t)}{t}$. אנחנו מקבלים בקירוב את המשוואה הדיפרנציאלית $\ln f(t) \sim -\int_1^{\sqrt{t}}\frac{f(x)}{x}dx$. $f(t) = \frac{1}{\ln t}$ הוא אכן פיתרון.

<u>שיקול 2:</u> נסמן ב־$P(x)$ את הסיכוי ש־x ראשוני. נרצה להביע את $P(x+1)$ בעזרת $P(x)$. אם x לא ראשוני, אז כנראה ש־$P(x+1), P(x)$ מאוד קרובים - כי יש עליהם את אותן דרישות (לא מתחלקים בראשוניים עד x). אם x ראשוני, צריך להתחמק מהאפשרות ש־$x+1$ מתחלק ב־x, כלומר להכפיל את $P(x)$ ב־$1-\frac{1}{x}$. נקבל:

$$P(x+1) = P(x)(P(x)(1-\tfrac{1}{x})) + (1-P(x))P(x) = P(x)(1-\tfrac{P(x)}{x})$$

אם נקרב $P(x+1) \approx P(x) + P'(x)$, נקבל $P'(x) = -P^2(x)/x$. $P(x) = \frac{1}{\ln x}$ אכן פיתרון!

4. זהות צ'בישב ופוסטולט ברטרן

לא סיימנו עם $n!$ כלל. נוכיח את הזהות הנהדרת הבאה:

$$\sum_{i\ge1}\psi(\frac{n}{i}) \quad = \quad \ln(n!)$$

<u>הוכחה:</u> ניזכר ש־$\psi(n) = \sum_{p^k\le n}\ln p$. אגף שמאל הוא $\sum_p \ln p\sum_{k\ge1}\lfloor\frac{n}{p^k}\rfloor = \sum_p \ln p\sum_{i,k:ip^k\le n}1 = \sum_{i,p^k:p^k\le\frac{n}{i}}\ln p$, והזהות נובעת מהפירוק של $n!$. ■

רואים כאן ממש טוב את האינטואיציה ל־PNT: אם $\psi(x)$ היא x בקירוב (זה בדיוק משפט ה־PNT), אז אגף שמאל הוא בקירוב $\sum_{i\ge1}\frac{n}{i} = n\ln n + O(n)$, וזה מסתדר עם אגף שמאל שהוא $n\ln n + O(n)$. אבל זו לא הוכחה, ומסתבר שנוסחה זו לבדה לא מספיקה להוכחה. אבל היא תיתן לנו לא מעט.

נסמן $T(n) := \ln(n!)$, ונתחיל לשחק עם הזהות $\sum_{i\ge1}\psi(\frac{n}{i}) = T(n)$.

- ניסיון ראשון - נסתכל על $T(n)-2T(\frac{n}{2})$ (שקול לבחינת המקדם הבינומי $\binom{2n}{n}$ שכבר הופיע, פשוט מנוסח אחרת).

מצד אחד, מבייבי סטרילינג, הוא שווה ל-$n\ln 2+O(\ln n)$. מצד שני, מזהות צ'בישב, הוא שווה ל-$\psi(n)-\psi(\frac{n}{2})+\psi(\frac{n}{3})\mp\cdots$. בגלל שהסימנים מתחלפים ו-ψ מונוטונית עולה, נקבל:

$$\psi(n)\geq T(n)-2T(\tfrac{n}{2})$$

וזה נותן לנו ש-$\vartheta(n)=\psi(n)+O(\sqrt{n})\geq n\ln 2+O(\sqrt{n})$, מה שגורר $\pi(x)=\Omega(\frac{x}{\ln x})$ (עם קבוע קרוב ל-$\ln 2$ כרצוננו). זה משלים את ההוכחה לכך ש-$\pi(x)=\vartheta(x)$ (הכיוון השני, שכבר ראינו, בעצם נובע מ-$T(n)-2T(\frac{n}{2})\geq\psi(n)-\psi(\frac{n}{2})$).

ננסה כעת להסיק את **פוסטולט ברטרן**: $\forall x>2:\pi(x)-\pi(\frac{x}{2})>0$, או באופן שקול: $\vartheta(x)>\vartheta(\frac{x}{2})$. נשים לב שאם $cx(1+o(1))\leq\vartheta(x)\leq Cx(1+o(1))$ אז $\vartheta(x)-\vartheta(\frac{x}{2})\geq(C-\frac{c}{2})x(1+o(1))$. לכן אם נצליח למצוא קבועים C,c כך ש-$C>\frac{c}{2}$, נסיים. עם זאת, אצלנו $C=\ln 4,c=\ln 2$ - לא עובד! צריך רעיון חדש.

נחזור לסכום המתחלף $\psi(n)-\psi(\frac{n}{2})+\psi(\frac{n}{3})\mp\cdots$. ניקח **3** איברים הפעם:
$T(n)-2T(\frac{n}{2})\leq\psi(n)-\psi(\frac{n}{2})+\psi(\frac{n}{3})$, כלומר:

$$\psi(n)-\psi(\tfrac{n}{2})\geq n\ln 2+O(\ln n)-\psi(\tfrac{n}{3})\geq n\ln 2-\ln 4\tfrac{n}{3}+O(\ln n)$$

בזכות זה ש-$\vartheta(n)=\psi(n)+O(\sqrt{n})$ ו-$\ln 2>\frac{1}{3}\ln 4$, נובע ש-$\vartheta(n)-\vartheta(\frac{n}{2})\geq\frac{\ln 2}{3}n+O(\sqrt{n})$, ועבור n גדול מספיק הפוסטולט נובע!

כלומר קיבלנו 3 תוצאות מעניינות ע"י זה שלקחנו איבר אחד, שני איברים, ושלושה איברים ראשונים בסכום...

- ניסיון הכללה - נסתכל על $S(n)=\sum T(\frac{n}{a_i})-\sum T(\frac{n}{b_j})$ (שקול לבחינת המנה $\frac{\prod(\frac{n}{a_i})!}{\prod(\frac{n}{b_j})!}$)

מבייבי סטירלינג, $T(\frac{n}{a})=\frac{n}{a}\ln n-\frac{\ln a}{a}n+O(\ln n)$. אנחנו רוצים שב-$S(n)$ יהיו רק גורמים לינאריים, לכן נדרוש $\sum\frac{1}{a_i}=\sum\frac{1}{b_j}$. נקבל: $S(n)=n(\sum\frac{\ln b_j}{b_j}-\sum\frac{\ln a_i}{a_i})+O(\ln n)$. בנוסף, נשמח אם ב-$S(n)=$ $(\sum_i\psi(\frac{n}{ka_i})-\sum_j\psi(\frac{n}{kb_j}))$ יהיו סימנים מתחלפים לאחר קיבוץ איברים. מסתבר שהבחירה הקסומה הבאה טובה במיוחד:

$$(a_1,a_2)=(1,\tfrac{1}{30}),(b_1,b_2,b_3)=(\tfrac{1}{2},\tfrac{1}{3},\tfrac{1}{5})$$

נקבץ איברים בסכום. כדי לדעת כמה פעמים $\psi(\frac{n}{k})$ מופיע, צריך לספור כמה פעמים k מתחלק באיברי $(a_i)_i$ פחות כמה פעמים מתחלק באיברי $(b_j)_j$. קיצורי דרך לחישוב:

- תלוי רק ב-$\gcd(k,30)$ (30 הוא ה-LCM של $1,2,3,5,30$)
- סימטרי ביחד ל-15 ($k,30-k$ יופיעו עם אותו מקדם)
- אם $\gcd(k,30)=1$ המקדם הוא 1

נקבל:

$$\psi(x)-\psi(\tfrac{x}{6})+\psi(\tfrac{x}{7})-\psi(\tfrac{x}{10})+\psi(\tfrac{x}{11})-\psi(\tfrac{x}{12})+\psi(\tfrac{x}{13})-\psi(\tfrac{x}{15})\pm\cdots=cx+O(\ln x)$$

כאשר $c=\frac{\ln 2}{2}+\frac{\ln 3}{3}+\frac{\ln 5}{5}-\frac{\ln 1}{1}-\frac{\ln 30}{30}\approx 0.921>0$. הסימנים המתחלפים הם נס, אבל הם משחקים לטובתינו - הסימנים והמונוטוניות נותנים:

$$\psi(x) - \psi(\tfrac{x}{6}) \le cx + O(\ln x) \le \psi(x)$$

או:

$$\vartheta(x) - \vartheta(\tfrac{x}{6}) \le cx + O(\sqrt{x}) \le \vartheta(x)$$

ע"י הצבה של $x, \frac{x}{6}, \frac{x}{6^2}, \cdots$, נקבל:

$$cx + O(\sqrt{x}) \le \vartheta(x) \le c(1 + \tfrac{1}{6} + \tfrac{1}{6^2} + \cdots)x + O(\sqrt{x})$$

<u>מסקנה:</u> $cx + O(\sqrt{x}) \le \vartheta(x) \le \frac{6}{5}cx + O(\sqrt{x})$, עם $c \approx 0.921, C := \frac{6}{5}c \approx 1.105$. בפרט, $\vartheta((1+\varepsilon)x) - \vartheta(x) \ge (\varepsilon - \frac{1}{5})x + O(\sqrt{x})$, ולכן לכל $\varepsilon > \frac{1}{5}$ מתקיים: יש x_ε כך שבכל קטע מהצורה $[x, x(1+\varepsilon)]$ עם $x > x_\varepsilon$ יש ראשוני, ולמעשה - כמות ראשוניים ששואפת לאינסוף עם x כמו $\frac{x}{\ln x}$. ($x_\varepsilon = O(\frac{1}{(\varepsilon - \frac{1}{5})^2})$.)

<u>הערה 1:</u> בהנחת ה-PNT, זה נכון **לכל** $\varepsilon > 0$, אבל קשה לקבל חסם על x_ε.

<u>הערה 2:</u> בהנחת ה-PNT, ארדש ודיאמונד הראו שאפשר להכליל את הרעיונות של צ'בישב ולקבל חסמים קרובים כרצוננו מהצורה $\vartheta(x) \in [(1-\varepsilon)x, (1+\varepsilon)x]$.

<u>הערה 3:</u> $\frac{(30n)!n!}{(10n)!(6n)!(15n)!}$, שהוא $\frac{\prod(\frac{n}{a_i})!}{\prod(\frac{n}{b_j})!}$ לאחר מכנה משותף, יוצא תמיד שלם! זה #נס, ולא נובע מהדרישה $\sum \frac{1}{b_j} = \sum \frac{1}{a_i}$. עד היום לא מצאו את כל הביטויים $\frac{\prod(\frac{n}{a_i})!}{\prod(\frac{n}{b_j})!}$ שיוצאים שלמים, חוץ מהמקרים שבמכנה יש איבר אחד יותר מהמונה (ועשו זאת רק ב-2009), כמו בשני המקרים שראינו. לפי ההערה הקודמת ביטויים כאלה יעזרו למצוא הוכחה ל-PNT או אפילו להשערת רימן.

<u>הערה 4:</u> אפשר להכליל את פוסטולט ברטרן בעוד כיוון. סילבסטר ושור הוכיחו באופן בלתי תלוי את המשפט הבא, שידוע בתור **משפט סילבסטר**: בהינתן k מספרים עוקבים גדולים מ-k, לאחד מהם לפחות יש גורם ראשוני גדול מ-k. במילים אחרות, אם $n \ge 2k$ אז ל-$\binom{n}{k}$ גורם ראשוני גדול מ-k. אם ניקח $n = 2k$ נקבל את הפוסטולט. למשפט זה יש שימושים במשוואות דיופנטיות ($\binom{n}{k} = a^b$ לא פתיר עם $b > 1$ ו-$k \in [4, n-4]$) ובאי-פריקות של פולינומים (כמו $\sum_{i=0}^{n} \frac{a_i}{i!}x^i, a_0 = a_n = 1$).